(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平7－162451

(43)公開日　平成7年（1995）6月23日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/54					
	12/58					
Ｇ０６Ｆ	13/00	３５１　Ｇ	7368－5B			
			8732－5K	Ｈ０４Ｌ 11/20	１０１	Ｂ
			8724－5L	Ｇ０６Ｆ 15/21		Ｚ

審査請求　未請求　請求項の数7　ＯＬ（全 20 頁）　最終頁に続く

(21)出願番号　特願平5－311505

(22)出願日　平成5年（1993）12月13日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72)発明者　大畑　秀雄
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　秋田　収喜

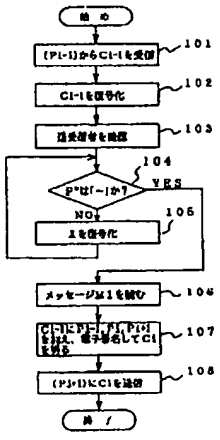
(54)【発明の名称】電子回覧方式

(57)【要約】

【目的】　回覧経路情報の改ざんや回覧途中の情報追加に対処した電子回覧方式を提供すること。

【構成】　通信回線を通し複数者間でメッセージデータを順送りに回覧する電子回覧方式において、回覧開始者は、メッセージデータに、現回覧者と次回覧者の識別子を加えたデータに電子署名して署名付通信データとし、前記署名付通信データを次回覧者に送り、途中回覧者は、前回覧者の識別子を基に、前回覧者から受信した署名付通信データを順次復号して、前記前回覧者から受信した署名付通信データ中の回覧開始者からのメッセージデータを読み、また、途中回覧者は、前記前回覧者から受信した署名付通信データに、前回覧者、現回覧者、および次回覧者の識別子を加えたデータに電子署名して送信用の署名付通信データとし、前記送信用の署名付通信データを次回覧者に送る。

図 4



1

【特許請求の範囲】

【請求項1】　通信回線を通し複数者間でメッセージデータを順送りに回覧する電子回覧方式において、回覧開始者は、メッセージデータに、現回覧者と次回覧者の識別子を加えたデータに電子署名して署名付通信データとし、前記署名付通信データを次回覧者に送り、途中回覧者は、前回覧者の識別子を基に、前回覧者から受信した署名付通信データを順次復号して、前記前回覧者から受信した署名付通信データ中の回覧開始者からのメッセージデータを読み、また、途中回覧者は、前記前回覧者から受信した署名付通信データに、前回覧者、現回覧者、および次回覧者の識別子を加えたデータに電子署名して送信用の署名付通信データとし、前記送信用の署名付通信データを次回覧者に送ることを特徴とする電子回覧方式。

【請求項2】　通信回線を通し複数者間でメッセージデータを順送りに回覧する電子回覧方式において、回覧開始者は、メッセージデータに電子署名したデータと、現回覧者と次回覧者の識別子とからなる回覧経路を示すデータに電子署名したデータとを加えて署名付通信データとし、前記署名付通信データを次回覧者に送り、途中回覧者は、前回覧者の識別子を基に、前回覧者から受信した署名付通信データの中の回覧経路を示すデータを順次を復号して、回覧開始者を判定し、回覧開始者の識別子を基に、前記前回覧者から受信した署名付通信データ中の回覧開始者からのメッセージデータを復号して、メッセージデータを読み、また、途中回覧者は、前記前回覧者から受信した署名付通信データ中の回覧経路を示すデータに、前回覧者、現回覧者、および次回覧者の識別子を加えたデータに電子署名したデータと、前記回覧開始者がメッセージデータに電子署名したデータとを加えて送信用の署名付通信データとし、前記送信用の署名付通信データを次回覧者に送ることを特徴とする電子回覧方式。

【請求項3】　通信回線を通し複数者間でメッセージデータを順送りに回覧する電子回覧方式において、回覧開始者は、メッセージデータに、現回覧者と次回覧者の識別子を加えたデータに電子署名して署名付通信データとし、前記署名付通信データを次回覧者に送信し、途中回覧者は、前回覧者の識別子を基に、前回覧者から受信した署名付通信データを順次復号して、前記署名付通信データ中の回覧開始者および途中回覧者からのメッセージデータを読み、また、途中回覧者は、前記前回覧者から受信した署名付通信データに、途中回覧者が作成したメッセージデータと、前回覧者、現回覧者、および次回覧者の識別子とを加えたデータに電子署名して送信用の署名付通信データとし、前記送信用の署名付通信データを次回覧者に送ることを特徴とする電子回覧方式。

【請求項4】　通信回線を通し複数者間でメッセージデータを順送りに回覧する電子回覧方式において、回覧開

2

始者は、メッセージデータに電子署名したデータと、現回覧者と次回覧者の識別子とからなる回覧経路を示すデータに電子署名したデータとを加えて署名付通信データとし、前記署名付通信データを次回覧者に送り、途中回覧者は、前回覧者の識別子を基に、前回覧者からの前記署名付通信データの中の回覧経路を示すデータを順次を復号して、前記署名付通信データ中の回覧開始者から途中回覧者までの回覧者を判定し、前記回覧開始者から途中回覧者までの回覧者の識別子を基に、前記署名付通信データ中の回覧開始者から途中回覧者までの回覧者からのメッセージデータを読み、また、途中回覧者は、前回覧者からの前記署名付通信データの中の回覧経路を示すデータに、前回覧者、現回覧者、および次回覧者の識別子を加えたデータに電子署名したデータと、途中回覧者が作成したメッセージデータに電子署名したデータと、前回覧者からの前記署名付通信データの中の回覧開始者から途中回覧者までの各回覧者が各々作成したメッセージデータに電子署名したデータとを加えて送信用の署名付通信データとし、前記送信用の署名付通信データを次回覧者に送ることを特徴とする電子回覧方式。

【請求項5】　請求項1ないし請求項4のいずれか1項に記載された電子回覧方式において、次回覧者に署名付通信データを受け渡す際に、送信側回覧者が、送信用の署名付通信データを受信側回覧者の公開暗号鍵で暗号化して暗号化署名付通信データとし、前記暗号化署名付通信データを受信側回覧者に送り、受信側回覧者は、受信した前記暗号化署名付通信データを受信側回覧者の秘密暗号鍵で復号して署名付通信データを得ることを特徴とする電子回覧方式。

【請求項6】　請求項1ないし請求項4のいずれか1項に記載された電子回覧方式において、次回覧者に署名付通信データを受け渡す際に、送信側回覧者が、暗号鍵を生成して、送信用の署名付通信データを前記暗号鍵で暗号化して暗号化署名付通信データとし、前記暗号化署名付通信データを受信側回覧者に送り、受信側回覧者は、受信した前記暗号化署名付通信データに電子署名して受取署名付返信データとし、前記受取署名付返信データを前記送信側回覧者に返送し、前記送信側回覧者は、返送された前記受取署名付返信データを、前記受信側回覧者の識別子を基に復号して、復号されたデータがさきに送信した前記暗号化署名付通信データと相違しないことを確認した上で、復号鍵を前記受信側回覧者に送信するとともに、前記受取署名付返信データと前記復号鍵を保管し、前記受信側回覧者は、受信した前記復号鍵でさきに受信した暗号化署名付通信データを復号して署名付通信データを得ることを特徴とする電子回覧方式。

【請求項7】　請求項1ないし請求項6に記載のいずれかの電子回覧方式において、回覧に伴うデータの電子署名の際に、署名する回覧者の秘密暗号鍵で前記データを暗号化することにより署名することを特徴とする電子回

覧方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、通信回線を介して複数者間でメッセージデータを順送りに回覧する方式に関する。

【０００２】

【従来の技術】コンピュータネットワークの普及とともに、その上でオフィスの書類業務を電子的に処理するためのさまざまな技術開発が進められている。

【０００３】情報処理学会第３９回（平成元年後期）全国大会予稿集、２Ｕ－７「書類の回覧制御システムの試作」（１９８９年）第２０４７頁から第２０４８頁には、電子メールシステム上に実現した書類回覧システムでの回覧制御方法が記載されている。

【０００４】書類業務電子化を実現する上での大きな問題としてセキュリティ対策があるが、電子通信学会論文誌、「公開鍵暗号による高速かつ安全なディジタル署名法」、第Ｊ６７－Ｄ巻（１９８４年）第３０５頁から第３１２頁には、公開鍵暗号の電子署名により通信内容の改ざんを防止する方法が記載されれている。

【０００５】また、電子通信学会技術研究報告（情報セキュリティ）、ＩＳＥＣ９１－４４「電子メールシステムでの公開鍵暗号の適用とその一考察」（１９９２年）には、通信内容の盗聴を防止するため電子メールシステムにＲＳＡ公開鍵暗号を適用した例が記載されており、情報処理学会第４６回（平成５年前期）全国大会予稿集、１Ｍ－３「暗号化電子メールＰＥＭ（Ｐｒｉｖａｃｙ　ＥｎｈａｎｃｅｄＭａｉｌ）の実装と課題」（１９９３年）第１－９９頁から第１－１００頁には、電子メールシステムでの盗聴と改ざんを防止するために提案されているＰＥＭ方式を実装評価した例が記載されている。

【０００６】また、電子情報通信学会論文誌、「暗号を用いた内容証明・配達証明サービス」、第Ｊ７０－Ｄ巻（１９８７年）第４２３頁から第４３１頁には、公開鍵暗号と共通鍵暗号の組み合わせにより電子メールにおける内容証明・配達証明サービスを実現した例が記載されている。

【０００７】

【発明が解決しようとする課題】前記従来技術では、回覧の場合のセキュリティ対策、とくに改ざん防止について検討されていなかった。

【０００８】従来技術が対象としていた１対１の通信に対し回覧に固有な問題として、まず、メッセージ内容そのもの以外に回覧した経路情報の改ざんに対抗する必要がある。

【０００９】これは書類の回覧が内容に対する回覧者の同意や承認を伴うような場合とくに重要になる。

【００１０】回覧に固有なもうひとつの問題は、回覧途中での情報追加への対処がある。

【００１１】回覧者が回覧中の情報にメモやコメントの形で独自の情報をつけ加えるという状況は現実場面で少なくない。

【００１２】回覧者に対し、改ざんに対抗しながら、情報追加を許すことができなければならない。

【００１３】本発明は、前記従来技術の問題点を解決するためになされたものであり、本発明の目的は、電子回覧方式において、回覧経路情報の改ざんや回覧途中の情報追加に対処可能な技術を提供することにある。

【００１４】本発明の前記目的並びにその他の目的及び新規な特徴は、本明細書の記載及び添付図面によって明らかにする。

【００１５】

【課題を解決するための手段】前記目的を達成するために、本発明の（１）手段は、通信回線を通し複数者間でメッセージデータを順送りに回覧する電子回覧方式において、回覧開始者は、メッセージデータに、現回覧者と次回覧者の識別子を加えたデータに電子署名して署名付通信データとし、前記署名付通信データを次回覧者に送り、途中回覧者は、前回覧者の識別子を基に、前回覧者から受信した署名付通信データを順次復号して、前記前回覧者から受信した署名付通信データ中の回覧開始者からのメッセージデータを読み、また、途中回覧者は、前記前回覧者から受信した署名付通信データに、前回覧者、現回覧者、および次回覧者の識別子を加えたデータに電子署名して送信用の署名付通信データとし、前記送信用の署名付通信データを次回覧者に送ることを特徴。

【００１６】また、本発明の（２）の手段は、通信回線を通し複数者間でメッセージデータを順送りに回覧する電子回覧方式において、回覧開始者は、メッセージデータに電子署名したデータと、現回覧者と次回覧者の識別子とからなる回覧経路を示すデータに電子署名したデータとを加えて署名付通信データとし、前記署名付通信データを次回覧者に送り、途中回覧者は、前回覧者の識別子を基に、前回覧者から受信した署名付通信データの中の回覧経路を示すデータを順次を復号して、回覧開始者を判定し、回覧開始者の識別子を基に、前記前回覧者から受信した署名付通信データ中の回覧開始者からのメッセージデータを復号して、メッセージデータを読み、また、途中回覧者は、前記前回覧者から受信した署名付通信データ中の回覧経路を示すデータに、前回覧者、現回覧者、および次回覧者の識別子を加えたデータに電子署名したデータと、前記回覧開始者がメッセージデータに電子署名したデータとを加えて送信用の署名付通信データとし、前記送信用の署名付通信データを次回覧者に送ることを特徴とする。

【００１７】また、本発明の（３）の手段は、通信回線を通し複数者間でメッセージデータを順送りに回覧する電子回覧方式において、回覧開始者は、メッセージデー

タに、現回覧者と次回覧者の識別子を加えたデータに電子署名して署名付通信データとし、前記署名付通信データを次回覧者に送信し、途中回覧者は、前回覧者の識別子を基に、前回覧者から受信した署名付通信データを順次復号して、前記署名付通信データ中の回覧開始者および途中回覧者からのメッセージデータを読み、また、途中回覧者は、前記前回覧者から受信した署名付通信データに、途中回覧者が作成したメッセージデータと、前回覧者、現回覧者、および次回覧者の識別子とを加えたデータに電子署名して送信用の署名付通信データとし、前記送信用の署名付通信データを次回覧者に送ることを特徴とする。

【００１８】また、本発明の（４）の手段は、通信回線を通し複数者間でメッセージデータを順送りに回覧する電子回覧方式において、回覧開始者は、メッセージデータに電子署名したデータと、現回覧者と次回覧者の識別子とからなる回覧経路を示すデータに電子署名したデータとを加えて署名付通信データとし、前記署名付通信データを次回覧者に送り、途中回覧者は、前回覧者の識別子を基に、前回覧者からの前記署名付通信データの中の回覧経路を示すデータを順次を復号して、前記署名付通信データ中の回覧開始者から途中回覧者までの回覧者を判定し、前記回覧開始者から途中回覧者までの回覧者の識別子を基に、前記署名付通信データ中の回覧開始者から途中回覧者までの回覧者からのメッセージデータを読み、また、途中回覧者は、前回覧者からの前記署名付通信データの中の回覧経路を示すデータに、前回覧者、現回覧者、および次回覧者の識別子を加えたデータに電子署名したデータと、途中回覧者が作成したメッセージデータに電子署名したデータと、前回覧者からの前記署名付通信データの中の回覧開始者から途中回覧者までの各回覧者が各々作成したメッセージデータに電子署名したデータとを加えて送信用の署名付通信データとし、前記送信用の署名付通信データを次回覧者に送ることを特徴とする。

【００１９】また、本発明の（５）の手段は、前記（１）ないし（４）の手段において、次回覧者に署名付通信データを受け渡す際に、送信側回覧者が、送信用の署名付通信データを受信側回覧者の公開暗号鍵で暗号化して暗号化署名付通信データとし、前記暗号化署名付通信データを受信側回覧者に送り、受信側回覧者は、受信した前記暗号化署名付通信データを受信側回覧者の秘密暗号鍵で復号して署名付通信データを得ることを特徴とする。

【００２０】また、本発明の（６）の手段は、前記（１）ないし（４）の手段において、次回覧者に署名付通信データを受け渡す際に、送信側回覧者が、暗号鍵を生成して、送信用の署名付通信データを前記暗号鍵で暗号化して暗号化署名付通信データとし、前記暗号化署名付通信データを受信側回覧者に送り、受信側回覧者は、

受信した前記暗号化署名付通信データに電子署名して受取署名付返信データとし、前記受取署名付返信データを前記送信側回覧者に返送し、前記送信側回覧者は、返送された前記受取署名付返信データを、前記受信側回覧者の識別子を基に復号して、復号されたデータがさきに送信した前記暗号化署名付通信データと相違しないことを確認した上で、復号鍵を前記受信側回覧者に送信するとともに、前記受取署名付返信データと前記復号鍵を保管し、前記受信側回覧者は、受信した前記復号鍵でさきに受信した暗号化署名付通信データを復号して署名付通信データを得ることを特徴とする。

【００２１】また、本発明の（７）の手段は、前記（１）ないし（６）に手段おいて、回覧に伴うデータの電子署名の際に、署名する回覧者の秘密暗号鍵で前記データを暗号化することにより署名することを特徴とする。

【００２２】

【作用】前記手段によれば、回覧開始者あるいは途中回覧者が作成したメッセージデータに、前回覧者、現回覧者、および次回覧者の識別子を加えたデータに、各回覧者が電子署名したデータを、次回覧者に送信するようにしたので、第３者による経路の偽造を防止することが可能である。

【００２３】また、前記手段によれば、回覧開始者あるいは途中回覧者が作成したメッセージデータに、前記回覧開始者あるいは途中回覧者が電子署名したデータと、前回覧者、現回覧者、および次回覧者の識別子からなる回覧経路を示すデータに、各回覧者が電子署名したデータとを次回覧者に送信するようにしたので、第３者による経路の偽造を防止することが可能であるばかりでなく、さらに、電子署名に要する情報処理装置の処理時間を短縮することが可能である。

【００２４】また、前記手段によれば、各回覧者が電子署名したデータを、次回覧者に送信する際に、次回覧者の公開鍵で暗号化するようにしたので、第３者による経路の偽造を防止することが可能であるばかりでなく、さらに、盗聴を防止することが可能である。

【００２５】また、前記手段によれば、各回覧者が電子署名したデータを、次回覧者に送信する際に、送信側回覧者が、暗号鍵を生成して、前記送信側回覧者が電子署名したデータを前記暗号鍵で暗号化して、受信側回覧者に送り、受信側回覧者は、受信した暗号化されたデータに電子署名して、前記送信側回覧者に返送し、前記送信側回覧者は、返送された前記受信側回覧者が電子署名したデータを、前記受信側回覧者の識別子を基に復号して、前記電子署名したデータがさきに送信したものと相違しないことを確認した上で、復号鍵を前記受信側回覧者に送信するとともに、復号鍵と、前記受信側回覧者から返送された前記受信側回覧者が電子署名したデータとを保管し、前記受信側回覧者は、受信した前記復号鍵で

さきに受信した電子署名したデータを復号するようにしたので、第3者による経路の偽造を防止することが可能であるばかりでなく、さらに、第3者による経路の偽造があった場合に、その特定が容易になる。

【0026】

【実施例】以下、図面を参照して本発明の実施例を詳細に説明する。

【0027】なお、実施例を説明するための全図において、同一機能を有するものは同一符号を付け、その繰り返しの説明は省略する。

【0028】

【実施例1】図1は、本発明の実施例1である電子回覧方式を実現するシステムの概略構成を示す図である。

【0029】図1において、701は情報処理装置、702は入力装置、703は表示装置、704は通信回線インタフェース装置、705は通信回線である。

【0030】情報処理装置701は、回覧するメッセージデータの編集、回覧されたメッセージデータの表示、他情報処理装置とのデータの通信、利用者間のメッセージデータの回覧処理、セキュリティ保護のためのメッセージデータの暗号化・復号化計算処理、その他各種プログラムの実行処理などを行う。

【0031】入力装置702からは、回覧したいメッセージデータを入力したり、各種プログラムへのデータやコマンドなどが入力される。

【0032】表示装置703は、回覧されてきたメッセージデータを表示したり、各種プログラムの処理結果などを表示する。

【0033】各情報処理装置は、通信回線インタフェース装置704と通信回線705を介して、それぞれ他の情報処理装置との間でデータを通信する。

【0034】次に、以下の説明で使用する記号を説明する。

【0035】(Pi) (i＝1, 2, …) は、回覧経路上のi番目の回覧者、Pi (i＝1, 2, …) は、回覧経路上のi番目の回覧者の識別子を表し、回覧経路は回

$$C1 \equiv D1[M1:\text{—}:P1:P2]$$

本実施例1における、回覧者 (P1) の手順について図2を用いて説明する。

【0047】図2 (A) に示すように、回覧者 (P1) は、メッセージM1に、回覧の起点を表わす記号「—」、回覧元の回覧者の識別子P1、次回覧先の識別子P2を加えたデータ20を作成する。

【0048】そして、図2 (B) に示すように、それを回覧者 (P1) の秘密鍵で署名、即ち、暗号化する。これがC1であり、さらに、C1を数式で表したのが、前記(数1) 式である。

【0049】なお、図2 (B) において、P1は回覧元

$$E1[C1]=E1[D1[M1:\text{—}:P1:P2]]=M1:\text{—}:P1:P2 \quad \cdots (数2)$$

(b) C1復号結果中の識別子P1、P2が、それぞれ送覧開始前に確定し以後不変である場合であっても、また回覧者が次回覧者を選べる場合であってもよい。

【0036】Mi (i＝1, 2, …) は、回覧者 (Pi) が回覧情報として流すメッセージデータである。

【0037】Ei[X] (i＝1, 2, …) は、回覧者 (Pi) の公開鍵によるXの暗号化である。

【0038】Di[X] (i＝1, 2, …) は、回覧者 (Pi) の秘密鍵によるXの復号化またはXに対する署名である。

【0039】これらは公開鍵法による対の鍵であり、具体的にはRSA暗号などを使用する。

【0040】なお、公開鍵法においては、公開鍵により暗号化し、秘密鍵により復号化するのが普通であるので、前記Ei[X]は、回覧者 (Pi) の公開鍵によるXの暗号化、Di[X]は、回覧者 (Pi) の秘密鍵によるXの復号化と記載したが、回覧者Piの秘密鍵によりXを暗号化し、回覧者 (Pi) の公開鍵によりXを復号化することも可能である。

【0041】本実施例1、及び、後記する各実施例では、後者の回覧者 (Pi) の秘密鍵によりXを暗号化し、回覧者 (Pi) の公開鍵によりXを復号化する方法を使用する。

【0042】Ki[X] (i＝1, 2, …) は、回覧者 (Pi) の共通暗号鍵によるXの暗号化である。共通暗号鍵としては、DES暗号などを使用する。

【0043】まず、回覧元の回覧者 (P1) が発したメッセージM1を、回覧者 (P2) 、(P3) 、(P4) と順次回覧する具体的場面を想定して説明する。

【0044】各回覧者は順次以下の手順で通信する。

【0045】(1) 回覧者 (P1)

(a) メッセージM1に、回覧の起点を表わす記号「—」、回覧元の回覧者の識別子P1、次回覧先の識別子P2を加え、回覧者 (P1) の秘密鍵で署名したものをC1とし、回覧者P2にC1を送る。

【0046】

【数1】

$$\cdots (数1)$$

の回覧者の識別子、P2は次回覧先の識別子、「—」は回覧の起点を表わす記号、M1はメッセージを示しており、また、同図 (B) 、および、後記の図面において、散点パターンは電子署名されていることを示す。

【0050】回覧者 (P1) は、前記C1を次回覧者 (P2) に送信する。

【0051】(2) 回覧者 (P2)

(a) 受信したC1を回覧者 (P1) の公開鍵で復号化する。

【0052】

【数2】

受信者の回覧者の識別子と一致することを確認する。

9

【0053】（c）記号「－」から回覧者（P1）が回覧元であると判断し、メッセージM1を読む。

【0054】（d）C1に、前回覧者識別子P1、現回覧者識別子P2、次回覧者識別子P3を加え、回覧者（P

C2≡D2[C1:P1:P2:P3]

回覧者（P2）の手順について図3を用いて説明する。

【0056】回覧者（P2）は、C1を受信したら、図2（B）に示す、前回覧者（P1）が、メッセージM1に、回覧の起点を表わす記号「－」、回覧元の回覧者の識別子P1、次回覧先の識別子P2を加えたデータを、回覧者（P1）の秘密鍵で署名、即ち、暗号化したC1を、前回覧者（P1）の公開鍵で復号化する。

【0057】これを数式で表したのが、前記（数2）式である。

【0058】次に、C1復号結果中の識別子P1、P2が、それぞれ送受信者の回覧者の識別子と一致することを確認し、記号「－」から回覧者（P1）が回覧元であると判断し、メッセージM1を読む。

【0059】次に、C1に、前回覧者識別子P1、現回覧者識別子P2、次回覧者識別子P3を加えたデータを作成

E2[C2]＝E2[D2[C1:P1:P2:P3]]＝C1:P1:P2:P3　…（数4）

（b）C2復号結果中の識別子P2、P3がそれぞれ送受信者の回覧者の識別子と一致することを確認する。

【0065】（c）C2復号結果中の識別子P1を識別子としてもつ回覧者の公開鍵でC1を復号化する。

【0066】

【数5】

E1[C1]＝E1[D1[M1:－:P1:P2]]＝M1:－:P1:P2　…（数5）

（d）記号「－」から回覧者（P1）が回覧元であると判断し、メッセージM1を読む。

【0067】（e）C2に、前回覧者識別子P2、現回覧者識別子P3、次回覧者識別子P4を加え、回覧者（P

C3≡D3[C2:P2:P3:P4]

（4）回覧者（P4）

（a）受信したC3を回覧者（P3）の公開鍵で復号化する。

E3[C3]＝E3[D3[C2:P2:P3:P4]]＝C2:P2:P3:P4　…（数7）

（b）C3復号結果中の識別子P3、P4がそれぞれ送受信者の回覧者の識別子と一致することを確認する。

【0070】（c）C3復号結果中の識別子P2を識別子としてもつ回覧者の公開鍵でC2を復号化する。

【0071】

【数8】

E2[C2]＝E2[D2[C1:P1:P2:P3]]＝C1:P1:P2:P3　…（数8）

（d）C2復号結果中の識別子P1を識別子としてもつ回覧者の公開鍵でC1を復号化する。

【0072】

【数9】

E1[C1]＝E1[D1[M1:－:P1:P2]]＝M1:－:P1:P2　…（数9）

（e）記号「－」から回覧者（P1）が回覧元であると判断し、メッセージM1を読む。

【0073】次に、一般の場合について途中回覧者（Pi）の手順を説明する。

【0074】回覧元の回覧者（P1）の手順は前記と同じである。

【0075】図4は、本実施例1の電子回覧方式における途中回覧者の処理手順を示すフローチャートである。

【0076】図4を用いて、本実施例1の電子回覧方式における途中回覧者の処理手順を説明する。

【0077】始めに、ステップ101で、前回覧者（Pi-1）からCi-1を受信し、ステップ102へ進む。

【0078】ステップ102では、Ci-1を前回覧者（Pi-1）の公開鍵で復号化し、その復号結果をX:P":P':Pとおいて、ステップ103へ進む。

【0079】ステップ103では、識別子P'が送信者である前回覧者（Pi-1）の識別子と、識別子Pが受信者である現回覧者（Pi）と一致することを確認し、ス

10

2）の秘密鍵で署名したものをC2とし、次回覧者（P3）にC2を送る。

【0055】

【数3】

…（数3）

する。

【0060】そして、図3に示すように、それを回覧者（P2）の秘密鍵で署名、即ち、暗号化する。これがC2であり、さらに、C2を数式で表したのが、前記（数3）式である。

【0061】回覧者（P2）は、次回覧者（P3）にC2を送信する。

【0062】以下、回覧者（P3）、（P4）も、同様な手順を繰り返す。

【0063】（3）回覧者（P3）

（a）受信したC2を回覧者（P2）の公開鍵で復号化する。

【0064】

【数4】

としてもつ回覧者の公開鍵でC1を復号化する。

【0068】

【数6】

…（数6）

【0069】

【数7】

としてもつ回覧者の公開鍵でC2を復号化する。

11

テップ１０４へ進む。

【００８０】ステップ１０４では、識別子P"が記号「－」であるかどうかを判定し、「－」であればステップ１０６へ進み、そうでなければステップ１０５へ進む。

【００８１】ステップ１０５では、識別子P"を識別子としてもつ回覧者の公開鍵でXを復号化し、その復号結果をあらためてX:P":P':Pとおいて、ステップ１０４に戻る。

【００８２】ステップ１０６に進んだ場合、XはメッセージM1であり、その内容を読んで、ステップ１０７へ進む。

【００８３】ステップ１０７では、Ci-1に、前回覧者識別子Pi-1、現回覧者識別子Pi、次回覧者識別子Pi+1を加え、現回覧者（Pi）の秘密鍵で署名したものをCi（≡Di[Ci-1:Pi-1:Pi:Pi+1]）として、ステップ１０８へ進む。

12

【００８４】ステップ１０８では、次回覧者（Pi+1）にCiを送信して、本手順を終了する。

【００８５】

【実施例２】本実施例２は、前記実施例１が必要とする繰返し復号化計算処理の負担を緩和したものである。

【００８６】本実施例２のシステム構成は、前記実施例１と同じである。

【００８７】回覧元の回覧者（P1）が発したメッセージM1を、回覧者（P2）、（P3）、（P4）と順次回覧する具体的場面を想定して説明する。

【００８８】各回覧者は順次以下の手順で通信する。

【００８９】（１）回覧者（P1）

（ａ）メッセージM1にメッセージ識別子ＭＩＤ1を加え、回覧者（P1）の秘密鍵で署名したものをCM1とする。

【００９０】

【数１０】

$$CM1\equiv D1[M1:MID1] \quad \cdots (数10)$$

（ｂ）メッセージ識別子ＭＩＤ1に、回覧の起点を表わす記号「－」、回覧元の回覧者の識別子P1、次回覧先の識別子P2を加え、回覧者（P1）の秘密鍵で署名したものをCR1とする。

【００９１】

【数１１】

$$CR1\equiv D1[MID1:-:P1:P2] \quad \cdots (数11)$$

（ｃ）CM1にCR1を加えたものをC1とし、次回覧者（P2）にC1を送る。

【００９２】

【数１２】

$$C1\equiv CM1:CR1 \quad \cdots (数12)$$

本実施例２における、回覧者（P1）の手順について図５を用いて説明する。

【００９３】回覧者（P1）は、図５（Ａ）に示すように、メッセージM1にメッセージ識別子ＭＩＤ1を付加したデータ３０を作成し、これを回覧者（P1）の秘密鍵で署名、即ち、暗号化する。これがCM1であり、さらに、CM1を数式で表したのが、前記（数１０）式である。

【００９４】また、回覧者（P1）は、メッセージ識別子ＭＩＤ1に、回覧の起点を表わす記号「－」、回覧元の回覧者の識別子P1、次回覧先の識別子P2を加えたデータを作成する。

【００９５】そして、図５（Ｂ）に示すように、それを回覧者（P1）の秘密鍵で署名、即ち、暗号化する。これがCR1であり、さらに、CR1を数式で表したのが、前記（数１１）式である。

【００９６】図５（Ｃ）に示すように、CM1にCR1を加えたものがC1であり、回覧者（P1）は、C1を次回覧者（P2）に送信する。

【００９７】また、C1を数式で表したのが、前記（数１２）である。

【００９８】（２）回覧者（P2）

（ａ）受信したC1中のCR1を回覧者（P1）の公開鍵で復号化する。

【００９９】

【数１３】

$$E1[CR1]=E1[D1[MID1:-:P1:P2]]$$
$$=MID1:-:P1:P2 \quad \cdots (数13)$$

（ｂ）CR1復号結果中の識別子P1、P2がそれぞれ送受信者の回覧者の識別子と一致することを確認する。

【０１００】（ｃ）記号「－」から識別子P1を識別子としてもつ回覧者（P1）が回覧元であると判断し、回覧者（P1）の公開鍵でC1中のCM1を復号化する。

【０１０１】

【数１４】

$$E1[CM1]=E1[D1[M1:MID1]]=M1:MID1 \quad \cdots (数14)$$

（ｄ）CR1復号結果とCM1復号結果中のメッセージ識別子ＭＩＤ1が一致することを確認し、メッセージM1を読む。

【０１０２】（ｅ）CR1に、前回覧者識別子P1、現回覧者識別子P2、次回覧者識別子P3を加え、回覧者（P2）の秘密鍵で署名したものをCR2とする。

【０１０３】

【数１５】

$$CR2\equiv D2[CR1:P1:P2:P3] \quad \cdots (数15)$$

13

(f) CM1にCR2を加えたものをC2とし、回覧者(P3)にC2を送る。

C2≡CM1:CR2

回覧者(P2)の手順について図6を用いて説明する。

【0105】回覧者(P2)は、C1を受信したら、図5(C)に示すC1の中のCR1を、前回覧者(P1)の公開鍵で復号化する。これを数式で表したのが、前記(数13)式である。

【0106】次に、CR1復号結果中の識別子P1、P2がそれぞれ送受信者の回覧者の識別子と一致することを確認し、記号「—」から識別子P1を識別子としてもつ回覧者(P1)が回覧元であると判断し、回覧者(P1)の公開鍵でC1中のCM1を復号化する。これを、数式で表したのが、前記(数14)である。

【0107】次に、CR1復号結果とCM1復号結果中のメッセージ識別子MID1が一致することを確認し、メッセージM1を読む。

【0108】次に、回覧者(P2)は、CR1に、前回覧者識別子P1、現回覧者識別子P2、次回覧者識別子P3

(b) CR2復号結果中の識別子P2、P3がそれぞれ送受信者の回覧者の識別子と一致することを確認する。

【0114】(c) CR2復号結果中の識別子P1を識別

(d) 記号「—」から識別子P1を識別子としてもつ回覧者(P1)が回覧元であると判断し、回覧者(P1)の公開鍵でC2中のCM1を復号化する。

E1[CM1]=E1[D1[M1:MID1]]=M1:MID1　…(数19)

(e) CR1復号結果とCM1復号結果中のメッセージ識別子MID1が一致することを確認し、メッセージM1を読む。

【0117】(f) CR2に、前回覧者識別子P2、現回

CR3≡D3[CR2:P2:P3:P4]　…(数20)

(g) CM1にCR3を加えたものをC3とし、回覧者(P4)にC3を送る。

C3≡CM1:CR3　…(数21)

(4) 回覧者(P4)

(a) 受信したC3中のCR3を回覧者(P3)の公開鍵で復号化する。

E3[CR3]=E3[D3[CR2:P2:P3:P4]]
=CR2:P2:P3:P4　…(数22)

(b) CR3復号結果中の識別子P3、P4がそれぞれ送受信者の回覧者の識別子と一致することを確認する。

【0121】(c) CR3復号結果中の識別子P2を識別

E2[CR2]=E2[D2[CR1:P1:P2:P3]]
=CR1:P1:P2:P3　…(数23)

(d) CR2復号結果中の識別子P1を識別子としてもつ回覧者の公開鍵でCR1を復号化する。

14

【0104】
【数16】

…(数16)

を加えたデータを作成し、そして、図6(A)に示すように、それを回覧者(P2)の秘密鍵で署名、即ち、暗号化する。これがCR2であり、さらに、CR2を数式で表したのが、前記(数15)式である。

【0109】図6(B)に示すように、CR2にCM1を加えたものがC2であり、C2を数式で表したのが、前記(数16)式である。

【0110】回覧者(P2)は、次回覧者(P3)にC2を送信する。

【0111】以下、回覧者(P3)、(P4)も、同様な手順を繰り返す。

【0112】(3) 回覧者(P3)

(a) 受信したC2中のCR2を回覧者(P2)の公開鍵で復号化する。

【0113】
【数17】

…(数17)

子としてもつ回覧者の公開鍵でCR1を復号化する。

【0115】
【数18】

…(数18)

【0116】
【数19】

覧者識別子P3、次回覧者識別子P4を加え、回覧者(P3)の秘密鍵で署名したものをCR3とする。

【0118】
【数20】

…(数20)

【0119】
【数21】

…(数21)

【0120】
【数22】

子としてもつ回覧者の公開鍵でCR2を復号化する。

【0122】
【数23】

…(数23)

【0123】
【数24】

15　　16

E1[CR1]=E1[D1[MID1:—:P1:P2]]
=MID1:—:P1:P2　　…（数24）

（e）記号「—」から識別子P1を識別子としてもつ回覧者（P1）が回覧元であると判断し、回覧者（P1）の公開鍵でC3中のCM1を復号化する。

【0124】
【数25】

E1[CM1]=E1[D1[M1:MID1]]=M1:MID1　　…（数25）

（f）CR1復号結果とCM1復号結果中のメッセージ識別子MID1が一致することを確認し、メッセージM1を読む。

【0125】次に、一般の場合について途中回覧者(Pi)の手順を説明する。

【0126】回覧元の回覧者（P1）の手順は前記と同様である。

【0127】図7は、本実施例2の電子回覧方式における途中回覧者の処理手順を示すフローチャートである。

【0128】図7を用いて、本実施例2の電子回覧方式における途中回覧者の処理手順を説明する。

【0129】始めに、ステップ201で、前回覧者（Pi-1）からCi-1（≡CM1:CRi-1）を受信し、ステップ202へ進む。

【0130】ステップ202では、Ci-1中のCRi-1を前回覧者（Pi-1）の公開鍵で復号化し、その復号結果をX:P":P':Pとおいて、ステップ203へ進む。

【0131】ステップ203では、識別子P'が送信者である前回覧者（Pi-1）の識別子と、識別子Pが受信者である現回覧者（Pi）の識別子と一致することを確認し、ステップ204へ進む。

【0132】ステップ204では、P"が記号「—」であるかどうかを判定し、「—」であればステップ206へ進み、そうでなければステップ205へ進む。

【0133】ステップ205では、識別子P"を識別子としてもつ回覧者の公開鍵でXを復号化し、その復号結果をあらためてX:P":P':Pとおいて、ステップ204に戻る。

【0134】ステップ206に進んだ場合は、識別子P'を持つ回覧者（P'）が回覧元であり、回覧者（P'）の公開鍵でCM1を以下のように復号化し、ステップ207へ進む。

【0135】
【数26】

E1[CM1]=E1[D1[M1:MID1]]=M1:MID1　　…（数26）

ステップ207では、ステップ206の復号結果中のMID1がXと一致することを確認し、メッセージM1を読んで、ステップ208へ進む。

【0136】ステップ208では、CRi-1に、前回覧者識別子Pi-1、現回覧者識別子Pi、次回覧者識別子Pi+1を加え、現回覧者（Pi）の秘密鍵で署名したものをCRi（≡Di[CRi-1:Pi-1:Pi:Pi+1]）として、ステップ209へ進む。

【0137】ステップ209では、CM1にCRiを加えたものをCi（≡CM1:CRi）として、ステップ210へ進む。

【0138】ステップ210では、次回覧者（Pi+1）にCiを送信して、本手順を終了する。

【0139】
【実施例3】本実施例3は、途中回覧者によるメッセージ追加に対処したものである。

【0140】メッセージの追加分は、具体的に、既回覧者のメッセージと独立なものであってもよいし、既回覧者のメッセージを修正したもの、あるいは、その修正後と修正前の差分データ出会ってもよい。

C1≡D1[—:M1:—:P1:P2]　　…（数27）

なお、本実施例3における前記回覧者（P1）手順は、メッセージM1に回覧の起点を表わす記号「—」が付与された以外は、前記実施例1の回覧者（P1）の手順と同じであるので説明は省略する。

【0141】本実施例3のシステム構成は、前記実施例1と同じである。

【0142】回覧元の回覧者（P1）がメッセージM1を回覧者（P2）に送り、回覧者（P2）はメッセージM1にメッセージM2を追加して回覧者（P3）に送り、回覧者（P3）はメッセージM1、M2にメッセージM3を追加して回覧者（P4）に送るという具体的場面を想定して説明する。

【0143】各回覧者は順次以下の手順で通信する。

【0144】（1）回覧者（P1）

（a）メッセージM1に、回覧の起点を表わす記号「—」、回覧元の回覧者の識別子P1、次回覧先の識別子P2を加え、回覧者（P1）の秘密鍵で署名したものをC1とし、回覧者（P2）にC1を送る。

【0145】
【数27】

（a）受信したC1を回覧者（P1）の公開鍵で復号化する。

【0146】（2）回覧者（P2）

【0147】
【数28】

E1[C1]=E1[D1[—:M1:—:P1:P2]]
=—:M1:—:P1:P2　　…（数28）

（b）C1復号結果中の識別子P1、P2がそれぞれ送受信者の回覧者の識別子と一致することを確認し、メッセージM1を読む。

【0148】（c）記号「—」から識別子P1をもつ回覧者（P1）が回覧元であることを判断する。

【0149】（d）C1に、メッセージM2、前回覧者識別子P1、現回覧者識別子P2、次回者識別子P3を加えたデータを作成する。

$$C2 \equiv D2[C1:M2:P1:P2:P3] \quad \cdots (数29)$$

前記回覧者（P2）の手順について図8を用いて説明する。

【0151】回覧者（P2）は、C1を受信したら、前回覧者（P1）の公開鍵で復号化する。

【0152】これを数式で表したのが、前記（数28）式である。

【0153】次に、C1復号結果中の識別子P1、P2が、それぞれ送受信者の回覧者の識別子と一致することを確認し、記号「—」から回覧者（P1）が回覧元であると判断し、メッセージM1を読む。

【0154】次に、C1に、メッセージM2、前回覧者識別子P1、現回覧者識別子P2、次回者識別子P3を加えたデータを作成する。

$$E2[C2]=E2[D2[C1:M2:P1:P2:P3]]$$
$$=C1:M2:P1:P2:P3 \quad \cdots (数30)$$

（b）C2復号結果中の識別子P2、P3がそれぞれ送受信者の回覧者の識別子と一致することを確認し、メッセージM2を読む。

【0160】（c）C2復号結果中の識別子P1を識別子としてもつ回覧者の公開鍵でC1を復号化し、メッセージM1を読む。

【0161】

【数31】

$$E1[C1]=E1[D1[—:M1:—:P1:P2]]$$
$$=—:M1:—:P1:P2 \quad \cdots (数31)$$

（d）記号「—」から識別子P1を持つ回覧者（P1）が回覧元であることを判断する。

【0162】（e）C2に、メッセージM3、前回覧者識別子P2、現回覧者識別子P3、次回覧者識別子P4を加え、回覧者（P3）の秘密鍵で署名したものをC3とし、回覧者（P4）にC3を送る。

【0163】

【数32】

$$C3 \equiv D3[C2:M3:P2:P3:P4] \quad \cdots (数32)$$

（4）回覧者（P4）

【0164】

【数33】

（a）受信したC3を回覧者（P3）の公開鍵で復号化する。

$$E3[C3]=E3[D3[C2:M3:P2:P3:P4]]$$
$$=C2:M3:P2:P3:P4 \quad \cdots (数33)$$

（b）C3復号結果中の識別子P3、P4がそれぞれ送受信者の回覧者の識別子と一致することを確認し、メッセージM3を読む。

【0165】（c）C3復号結果中の識別子P2を識別子としてもつ回覧者の公開鍵でC2を復号化し、メッセージM2を読む。

【0166】

【数34】

$$E2[C2]=E2[D2[C1:M2:P1:P2:P3]]$$
$$=C1:M2:P1:P2:P3 \quad \cdots (数34)$$

（d）C2復号結果中の識別子P1を識別子としてもつ回覧者の公開鍵でC1を復号化し、メッセージM1を読む。

【0167】

【数35】

$$E1[C1]=E1[D1[—:M1:—:P1:P2]]$$
$$=—:M1:—:P1:P2 \quad \cdots (数35)$$

（e）記号「—」から識別子P1をもつ回覧者（P1）が回覧元であることを判断する。

【0168】次に、一般の場合について途中回覧者（Pi）の手順を説明する。

【0150】

【数29】

【0155】そして、図8に示すように、それを回覧者（P2）の秘密鍵で署名、即ち、暗号化する。これがC2であり、さらに、C2を数式で表したのが、前記（数29）式である。

【0156】回覧者（P2）は、次回覧者（P3）にC2を送信する。

【0157】以下、回覧者（P3）、（P4）も、同様な手順を繰り返す。

【0158】（3）回覧者（P3）

（a）受信したC2を回覧者（P2）の公開鍵で復号化する。

【0159】

【数30】

【0169】回覧元の回覧者（P1）の手順は前記と同様である。

【0170】図9は、本実施例3の電子回覧方式における途中回覧者の処理手順を示すフローチャートである。

【0171】図9を用いて、本実施例3の電子回覧方式における途中回覧者の処理手順を説明する。

【0172】始めに、ステップ301で、前回覧者（Pi-1）からCi-1を受信し、ステップ302へ進む。

【0173】ステップ302では、Ci-1を前回覧者（Pi-1）の公開鍵で復号化し、その復号結果をX:M:P":P':Pとおいて、ステップ303へ進む。

【0174】ステップ303では、識別子P'が送信者である前回覧者（Pi-1）の識別子と、識別子Pが受信者である現回覧者（Pi）の識別子と一致することを確認し、ステップ304へ進む。

【0175】ステップ304では、メッセージMを読んで、ステップ305へ進む。

【0176】ステップ305では、Xと識別子P"が記号「—」であるかどうかを判定し、「—」であればステップ307へ進み、そうでなければステップ306へ進む。

【0177】ステップ306では、識別子P"を識別子としてもつ回覧者の公開鍵でXを復号化し、その復号結果をあらためてX:M:P":P':Pとおいて、ステップ304に戻る。

【0178】ステップ307では、Ci-1に、メッセージMi、前回覧者識別子Pi-1、現回覧者識別子Pi、次回覧者識別子Pi+1を加え、回覧者（Pi）の秘密鍵で署名したものをCi（≡Di[Ci-1:Mi:Pi-1:Pi:Pi+1]）として、ステップ308へ進む。

【0179】ステップ308では、次回覧者（Pi+1）にCiを送信して、本手順を終了する。

【0180】

【実施例4】本実施例4は、前記実施例2と実施例3の両方の利点を同時に実現したものである。

【0181】本実施例4のシステム構成は、前記実施例1と同じである。

【0182】前記実施例3と同様、回覧元の回覧者（P1）がメッセージM1を回覧者（P2）に送り、（P2）はメッセージM1にメッセージM2を追加して回覧者（P3）に送り、回覧者（P3）はメッセージM1、M2にメッセージM3を追加して回覧者（P4）に送るという具体的場面を想定して説明する。

【0183】各回覧者は順次以下の手順で通信する。

【0184】（1）回覧者（P1）

（a）メッセージM1にメッセージ識別子ＭＩＤ1を加え、回覧者（P1）の秘密鍵で署名したものをCM1とする。

【0185】

【数36】

$$CM1 \equiv D1[M1:MID1] \quad \cdots (数36)$$

（b）メッセージ識別子ＭＩＤ1に、回覧の起点を表わす記号「—」、回覧元の回覧者の識別子P1、次回覧先の識別子P2を加え、回覧者（P1）の秘密鍵で署名したものをCR1とする。

【0186】

【数37】

$$CR1 \equiv D1[—:MID1:—:P1:P2] \quad \cdots (数37)$$

（c）CM1にCR1を加えたものをC1とし、回覧者（P2）にC1を送る。

【0187】

【数38】

$$C1 \equiv CM1:CR1 \quad \cdots (数38)$$

なお、本実施例4における前記回覧者（P1）の手順は、回覧者（P1）の秘密鍵で署名したCR1中のメッセージ識別子ＭＩＤ1に、回覧の起点を表わす記号「—」を付与した以外は、前記実施例2の回覧者（P1）の手順と相違しないので説明は省略する。

【0188】（2）回覧者（P2）

（a）受信したC1中のCR1を回覧者（P1）の公開鍵で復号化する。

【0189】

【数39】

$$E1[CR1]=E1[D1[—:MID1:—:P1:P2]]$$
$$=—:MID1:—:P1:P2 \quad \cdots (数39)$$

（b）CR1復号結果中の識別子P1、P2がそれぞれ送受信者の回覧者の識別子と一致することを確認する。

【0190】（c）CR1復号結果中の識別子P1を識別子としてもつ回覧者（P1）の公開鍵でC1中のCM1を復号化する。

【0191】

【数40】

$$E1[CM1]=E1[D1[M1:MID1]]=M1:MID1 \quad \cdots (数40)$$

（d）CR1復号結果とCM1復号結果中のメッセージ識別子ＭＩＤ1が一致することを確認し、メッセージM1を読む。

【0192】（e）CR1復号結果中の記号「—」から識別子P1をもつ回覧者（P1）が回覧元であることを判断する。

【0193】（f）メッセージM2にメッセージ識別子ＭＩＤ2を加え、回覧者（P2）の秘密鍵で署名したものをCM2とする。

【0194】

【数４１】

$$CM2 \equiv D2[M2:MID2] \quad \cdots (数41)$$

（g）CR1に、メッセージ識別子ＭＩＤ2、前回覧者識別子P1、現回覧者識別子P2、次回覧者識別子P3を加え、回覧者（P2）の秘密鍵で署名したものをCR2とする。

【数４２】

$$CR2 \equiv D2[CR1:MID2:P1:P2:P3] \quad \cdots (数42)$$

（h）CM1にCM2とCR2を加えたものをC2とし、回覧者（P3）にC2を送る。

【数４３】

$$C2 \equiv CM1:CM2:CR2 \quad \cdots (数43)$$

前記回覧者（P2）の手順について説明する。

【０１９７】回覧者（P2）は、C1を受信したら、C1の中のCR1を、前回覧者（P1）の公開鍵で復号化する。これを数式で表したのが、前記（数３９）式である。

【０１９８】次に、CR1復号結果中の識別子P1、P2がそれぞれ送受信者の回覧者の識別子と一致することを確認し、記号「－」から識別子P1を識別子としてもつ回覧者（P1）が回覧元であると判断し、回覧者（P1）の公開鍵でC1中のCM1を復号化する。これを、数式で表したのが、前記（数４０）である。

【０１９９】次に、CR1復号結果とCM1復号結果中のメッセージ識別子ＭＩＤ1が一致することを確認し、メッセージM1を読む。

【０２００】次に、回覧者（P2）は、メッセージM2にメッセージ識別子ＭＩＤ2を加えたデータを作成し、それを回覧者（P2）の秘密鍵で署名、即ち、暗号化する。これがCM2であり、さらに、CM2を数式で表したのが、前記（数４１）式である。

$$E2[CR2]=E2[D2[CR1:MID2:P1:P2:P3]]$$
$$=CR1:MID2:P1:P2:P3 \quad \cdots (数44)$$

（b）CR2復号結果中の識別子P2、P3がそれぞれ送受信者の回覧者の識別子と一致することを確認する。

【０２０７】（c）CR2復号結果中の識別子P2を識別子としてもつ回覧者の公開鍵でC2中のCM2を復号化する。

$$E2[CM2]=E2[D2[M2:MID2]]=M2:MID2 \quad \cdots (数45)$$

（d）CR2復号結果とCM2復号結果中のメッセージ識別子ＭＩＤ2が一致することを確認し、メッセージM2を読む。

【０２０９】（e）CR2復号結果中の識別子P1を識別子としてもつ回覧者の公開鍵でCR1を復号化する。

$$E1[CR1]=E1[D1[－:MID1:－:P1:P2]]$$
$$=－:MID1:－:P1:P2 \quad \cdots (数46)$$

（f）CR1復号結果中の識別子P1を識別子としてもつ回覧者の公開鍵でC2中のCM1を復号化する。

【０２１１】

【数４７】

$$E1[CM1]=E1[D1[M1:MID1]]=M1:MID1 \quad \cdots (数47)$$

（g）CR1復号結果とCM1復号結果中のメッセージ識別子ＭＩＤ1が一致することを確認し、メッセージM1を読む。

【０２１２】（h）CR1復号結果中の記号「－」から識別子P1をもつ回覧者（P1）が回覧元であることを判断する。

【０２０１】つぎに、回覧者（P2）は、CR1に、前回覧者識別子P1、現回覧者識別子P2、次回覧者識別子P3を加えたデータを作成し、そして、それを回覧者（P2）の秘密鍵で署名、即ち、暗号化する。これがCR2であり、さらに、CR2を数式で表したのが、前記（数４２）式である。

【０２０２】図１０に示すように、CM1に、CM2とCR2とを加えたものがC2であり、C2を数式で表したのが、前記（数４３）式である。

【０２０３】回覧者（P2）は、次回覧者（P3）にC2を送信する。

【０２０４】以下、回覧者（P3）、（P4）も、同様な手順を繰り返す。

【０２０５】（3）回覧者（P3）

（a）受信したC2中のCR2を回覧者（P2）の公開鍵で復号化する。

【０２０６】

【数４４】

【０２０８】

【数４５】

子としてもつ回覧者の公開鍵でCR1を復号化する。

【０２１０】

【数４６】

【０２１３】（i）メッセージM3にメッセージ識別子ＭＩＤ3を加え、回覧者（P3）の秘密鍵で署名したものをCM3とする。

【０２１４】

【数４８】

CM3≡D3[M3:ＭＩD3] … (数48)

(j) CR2に、メッセージ識別子ＭＩD3、前回覧者識別子P2、現回覧者識別子P3、次回覧者識別子P4を加え、回覧者(P3)の秘密鍵で署名したものをCR3とする。

【0215】

【数49】

CR3≡D3[CR2:ＭＩD3:P2:P3:P4] … (数49)

【0216】

(k) CM1にCM2、CM3、CR3を加えたものをC3とし、回覧者(P4)にC3を送る。

【数50】

C3≡CM1:CM2:CM3:CR3 … (数50)

【0217】

(4) 回覧者(P4)

【数51】

(a) 受信したC3中のCR3を回覧者(P3)の公開鍵で復号化する。

E3[CR3]=E3[D3[CR2:ＭＩD3:P2:P3:P4]]
=CR2:ＭＩD3:P2:P3:P4 … (数51)

(b) CR3復号結果中の識別子P3、P4がそれぞれ送受信者の回覧者の識別子と一致することを確認する。

【0219】

【0218】 (c) CR3復号結果中の識別子P3を識別子としてもつ回覧者の公開鍵でC3中のCM3を復号化する

【数52】

E3[CM3]=E3[D3[M3:ＭＩD3]]=M3:ＭＩD3 … (数52)

(d) CR3復号結果とCM3復号結果中のメッセージ識別子ＭＩD3が一致することを確認し、メッセージM3を読む。

子としてもつ回覧者の公開鍵でCR1を復号化する。

【0221】

【0220】 (e) CR2復号結果中の識別子P1を識別

【数53】

E1[CR1]=E1[D1[—:ＭＩD1:—:P1:P2]]
=—:ＭＩD1:—:P1:P2 … (数53)

(f) CR1復号結果中のP1を識別子としてもつ回覧者の公開鍵でC3中のCM1を復号化する。

【0222】

【数54】

E1[CM1]=E1[D1[M1:ＭＩD1]]=M1:ＭＩD1 … (数54)

(g) CR1復号結果とCM1復号結果中のメッセージ識別子ＭＩD1が一致することを確認し、メッセージM1を読む。

1) を受信し、ステップ402へ進む。

【0223】 (h) CR1復号結果中の記号「—」から識別子P1をもつ回覧者(P1)が回覧元であることを判断する。

【0224】 次に、一般の場合について途中回覧者(Pi)の手順を説明する。

【0225】 回覧元の回覧者(P1)の手順は前記と同様である。

【0226】 図11は、本実施例4の電子回覧方式における途中回覧者の処理手順を示すフローチャートである。

【0227】 図11を用いて、本実施例4の電子回覧方式における途中回覧者の処理手順を説明する。

【0228】 始めに、ステップ401で、前回覧者(Pi-1)からCi-1 (≡CM1:CM2: ... :CMi-1:CRi-

【0229】 ステップ402では、Ci-1中のCRi-1を前回覧者(Pi-1)の公開鍵で復号化し、その復号結果をX:ＭＩD:P":P':Pとおいて、ステップ403へ進む。

【0230】 ステップ403では、識別子P'が送信者である前回覧者(Pi-1)の識別子と、識別子Pが受信者である現回覧者(Pi)の識別子と一致することを確認し、ステップ404へ進む。

【0231】 ステップ404では、kをi－1とおいて、ステップ405へ進む。

【0232】 ステップ405では、回覧者(Pk)の公開鍵でCMkを以下のように復号化し、ステップ406へ進む。

【0233】

【数55】

Ek[CMk]=Ek[Dk[Mk:ＭＩDk]]=Mk:ＭＩDk … (数55)

ステップ406では、ＭＩDとＭＩDkが一致することを確認し、メッセージMkを読んで、ステップ407へ進む。

【0234】 ステップ407では、XとP"が記号「—」であるかどうかを判定し、「—」であればステップ410へ進み、そうでなければステップ408へ進む。

【0235】 ステップ408では、識別子P"を識別子としてもつ回覧者の公開鍵でXを復号化し、その復号結果をあらためてX:ＭＩD:P":P':Pとおいて、ステッ

プ４０９へ進む。

【０２３６】ステップ４０９では、ｋをあらためてｋ－１とおいて、ステップ４０５に戻る。

【０２３７】ステップ４１０では、メッセージMiにメッセージ識別子ＭＩＤiを加え、現回覧者（Pi）の秘密鍵で署名したものをCMi（≡Di[Mi:ＭＩDi]）として、ステップ４１１へ進む。

【０２３８】ステップ４１１では、CRi-1に、メッセージ識別子ＭＩDi、前回覧者識別子Pi-1、現回覧者識別子Pi、次回覧者識別子Pi+1を加え、現回覧者（Pi）の秘密鍵で署名したものをCRi（≡Di[CRi-1:ＭＩDi:Pi-1:Pi:Pi+1]）として、ステップ４１２へ進む。

【０２３９】ステップ４１２では、CM1、CM2、...、CMi、CRiを加えたものをCi（≡CM1:CM2:...:CMi:CRi）として、ステップ４１３へ進む。

【０２４０】ステップ４１３では、次回覧者（Pi+1）にCiを送信して、本手順を終了する。

【０２４１】

【実施例５】本実施例５は、ある回覧者が既回覧経路情報を改ざんしたとき、その特定を容易とするものであり、それにより、改ざん防止効果を高めることができる。

【０２４２】本実施例５のシステム構成は、前記実施例１と同じである。

【０２４３】また、本実施例５は、前記実施例１ないし実施例４に適用することが可能である。

【０２４４】図１２は、本実施例５の電子回覧方式における回覧者間で通信データを受け渡す手順を示すフローチャートである。

【０２４５】図１２を用いて、本実施例５の電子回覧方式における回覧者間で通信データを受け渡す手順について説明する。

【０２４６】始めに、ステップ５０１では、送信側の現回覧者（Pi）が通信データCiを作成し、ステップ５０２へ進む。

【０２４７】ステップ５０２では、送信側の現回覧者（Pi）が、共通暗号鍵Kiを生成し、図１３に示すように、CiをKiで暗号化したものをCi'（≡Ki[Ci]）として、ステップ５０３へ進む。

【０２４８】ステップ５０３では、送信側の現回覧者（Pi）が受信側の次回覧者（Pi+1）にCi'を送って、ステップ５０４へ進む。

【０２４９】ステップ５０４では、受信側の次回覧者（Pi+1）が、図１３に示すように、受信したCi'に受信側の次回覧者（Pi+1）の秘密鍵で署名したものをCi"（≡Di+1[Ci']）として、ステップ５０５へ進む。

【０２５０】ステップ５０５では、受信側の次回覧者（Pi+1）が送信側の現回覧者（Pi）にCi"を返送して、ステップ５０６へ進む。

【０２５１】ステップ５０６では、送信側の現回覧者（Pi）が、返送されたCi"を受信側の次回覧者（Pi+1）の公開鍵で以下のように復号化し、ステップ５０７へ進む。

【０２５２】

【数５６】

$$Ei+1[Ci"]=Ei+1[Di+1[Ci']]=Ci' \quad \cdots (数５６)$$

ステップ５０７では、送信側の現回覧者（Pi）が、ステップ５０６の復号結果とステップ５０３で送ったCi'とが一致することを確認できたら、受信側の次回覧者（Pi+1）に共通暗号鍵Kiを送り、ステップ５０８へ進む。

【０２５３】ステップ５０８では、送信側の現回覧者（Pi）がCi"とKiを保管して、ステップ５０９へ進む。

【０２５４】ステップ５０９では、受信側の次回覧者（Pi+1）が、ステップ５０４で受け取ったCi'を受信したKiで以下のように復号化し、ステップ５１０へ進む。

【０２５５】

【数５７】

$$Ki[Ci']=Ki[Ki[Ci]]=Ci \quad \cdots (数５７)$$

ステップ５１０では、受信側の次回覧者（Pi+1）がCiを得て、本手順を終了する。

【０２５６】

【実施例６】本実施例６は、回覧者間の盗聴を防止するためのものである。

【０２５７】本実施例のシステム構成は、前記実施例１と同じである。

【０２５８】また、本実施例６は、前記実施例１ないし実施例４に適用することが可能である。

【０２５９】図１４は、本実施例６の電子回覧方式における回覧者間で通信データを受け渡す手順を示すフローチャートである。

【０２６０】図１４を用いて、本実施例６の電子回覧方式における回覧者間で通信データを受け渡す手順について説明する。

【０２６１】始めに、ステップ６０１で、送信側の現回覧者（Pi）がCiを作成し、ステップ６０２へ進む。

【０２６２】ステップ６０２では、図１５に示すように、送信側の現回覧者（Pi）が受信側の次回覧者（Pi+1）の公開鍵でCiを暗号化したものをCi'（≡Ei+1[Ci]）として、ステップ６０３へ進む。

【０２６３】ステップ６０３では、送信側の現回覧者（Pi）が受信側の次回覧者（Pi+1）にCi'を送って、ステップ６０４へ進む。

【0264】ステップ604では、受信側の次回覧者（Pi+1）が、受信したCi'を受信側の次回覧者（Pi+1）の秘密鍵で以下のように復号化し、ステップ605

Di+1[Ci']=Di+1[Ei+1[Ci]]=Ci　…（数58）

ステップ605では、受信側の次回覧者（Pi+1）がCiを得て、本手順を終了する。

【0266】以上、本発明を実施例に基づき具体的に説明したが、本発明は、前記実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更し得ることは言うまでもない。

【0267】

【発明の効果】以上説明したように、本発明によれば、回覧開始者あるいは途中回覧者が作成したメッセージデータに、前回覧者、現回覧者、および次回覧者の識別子を加えたデータに、各回覧者が電子署名したデータを、次回覧者に送信するようにしたので、第3者による経路の偽造を防止することが可能である。

【0268】また、本発明によれば、回覧開始者あるいは途中回覧者が作成したメッセージデータに、前記回覧開始者あるいは途中回覧者が電子署名したデータと、前回覧者、現回覧者、および次回覧者の識別子からなる回覧経路を示すデータに、各回覧者が電子署名したデータとを次回覧者に送信するようにしたので、第3者による経路の偽造を防止することが可能であるばかりでなく、さらに、電子署名に要する情報処理装置の処理時間を短縮することが可能である。

【0269】また、本発明によれば、各回覧者が電子署名したデータを、次回覧者に送信する際に、次回覧者の公開鍵で暗号化するようにしたので、第3者による経路の偽造を防止することが可能であるばかりでなく、さらに、盗聴を防止することが可能である。

【0270】また、本発明によれば、各回覧者が電子署名したデータを、次回覧者に送信する際に、送信側回覧者が、暗号鍵を生成して、前記送信側回覧者が電子署名したデータを前記暗号鍵で暗号化して、受信側回覧者に送り、受信側回覧者は、受信した暗号化されたデータに電子署名して、前記送信側回覧者に返送し、前記送信側回覧者は、返送された前記受信側回覧者が電子署名したデータを、前記受信側回覧者の識別子を基に復号して、前記電子署名したデータがさきに送信したものと相違しないことを確認した上で、復号鍵を前記受信側回覧者に送信するとともに、復号鍵と、前記受信側回覧者から返送された前記受信側回覧者が電子署名したデータとを保管し、前記受信側回覧者は、受信した前記復号鍵でさきに受信した電子署名したデータを復号するようにしたので、第3者による経路の偽造を防止することが可能であるばかりでなく、さらに、第3者による経路の偽造があった場合に、その特定が容易になる。

【図面の簡単な説明】

【図1】　本発明の実施例1である電子回覧方式を実現するシステムの概略構成を示す図である。

【図2】　本発明の実施例1における回覧元の回覧者の回覧者が作成するデータ、および電子署名したデータを説明するための図である。

【図3】　本発明の実施例1における2番目の回覧者が電子署名したデータを説明するための図である。

【図4】　本発明の実施例1における途中回覧者の処理手順を示すフローチャートである。

【図5】　本発明の実施例2における回覧元の回覧者の回覧者が作成するデータ、および電子署名したデータを説明するための図である。

【図6】　本発明の実施例2における2番目の回覧者が電子署名したデータを説明するための図である。

【図7】　本発明の実施例2における途中回覧者の処理手順を示すフローチャートである。

【図8】　本発明の実施例3における2番目の回覧者が電子署名したデータを説明するための図である。

【図9】　本発明の実施例3における途中回覧者の処理手順を示すフローチャートである。

【図10】　本発明の実施例4における2番目の回覧者が電子署名したデータを説明するための図である。

【図11】　本発明の実施例4における途中回覧者の処理手順を示すフローチャートである。

【図12】　本発明の実施例5における回覧者間で通信データを受け渡す手順を示すフローチャートである。

【図13】　本発明の実施例5における回覧者間で通信データを受け渡す際の暗号化を説明するための図である。

【図14】　本発明の実施例6における回覧者間で通信データを受け渡す手順を示すフローチャートである。

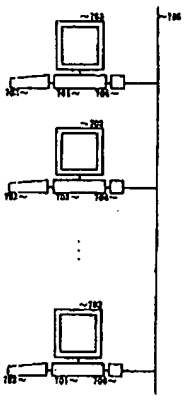
【図15】　本発明の実施例6における回覧者間で通信データを受け渡す際の暗号化を説明するための図である。

【符号の説明】

701…計算処理装置、702…入力装置、703…表示装置、704…通信回線インタフェース装置、705…通信回線。

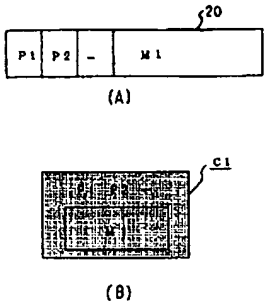
【図1】

図 1



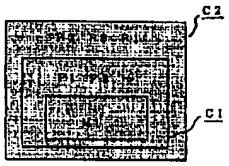
【図2】

図 2



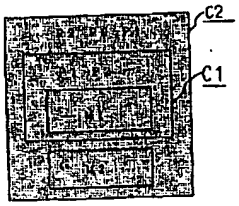
【図3】

図 3



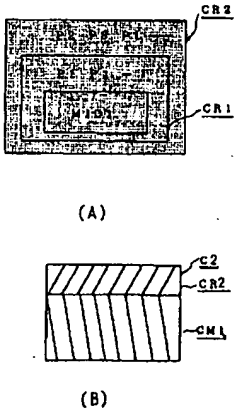
【図8】

図 8



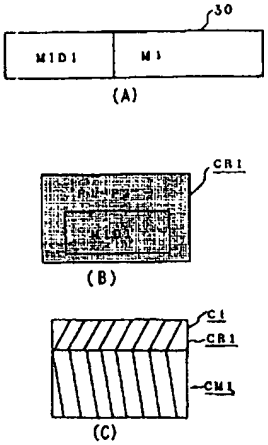
【図6】

図 6



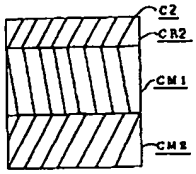
【図5】

図 5



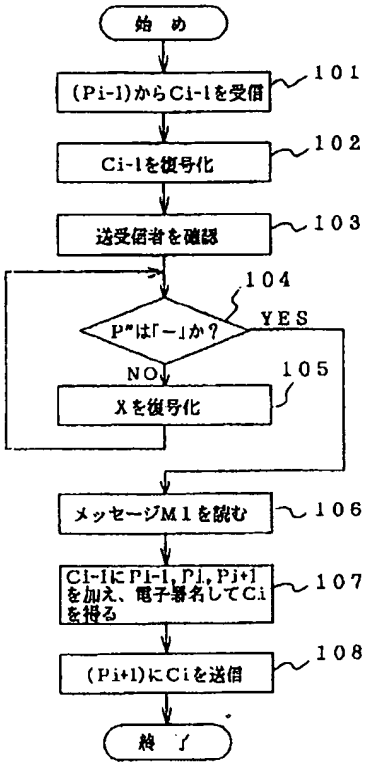
【図10】

図 10



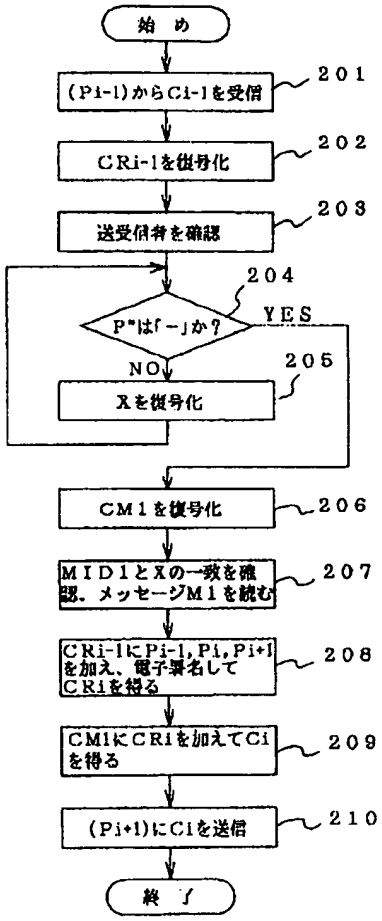
【図4】

図 4


始 め
(Pi-1)からCi-1を受信
101
Ci-1を復号化
102
送受信者を確認
103
104
P"は「－」か？
YES
NO
105
Xを復号化
メッセージM1を読む
106
Ci-1にPi-1, Pi, Pi+1を加え、電子署名してCiを得る
107
(Pi+1)にCiを送信
108
終 了

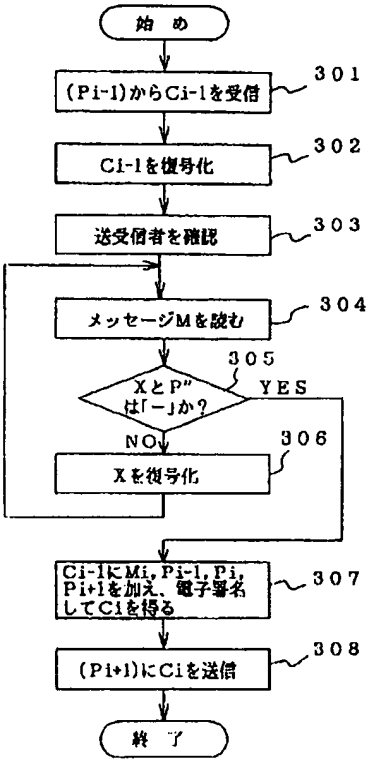
【図7】

図 7


始 め
(Pi-1)からCi-1を受信
201
CRi-1を復号化
202
送受信者を確認
203
204
P"は「－」か？
YES
NO
205
Xを復号化
CM1を復号化
206
MID1とXの一致を確認、メッセージM1を読む
207
CRi-1にPi-1, Pi, Pi+1を加え、電子署名してCRiを得る
208
CM1にCRiを加えてCiを得る
209
(Pi+1)にCiを送信
210
終 了

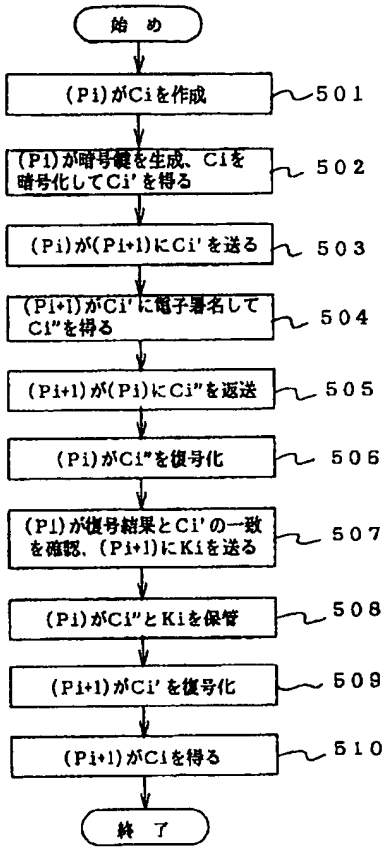
【図9】

図 9


始 め
(Pi-1)からCi-1を受信
301
Ci-1を復号化
302
送受信者を確認
303
メッセージMを読む
304
XとP"は「－」か？
305
YES
NO
X を復号化
306
Ci-1にMi, Pi-1, Pi, Pi+1を加え、電子署名してCiを得る
307
(Pi+1)にCiを送信
308
終 了

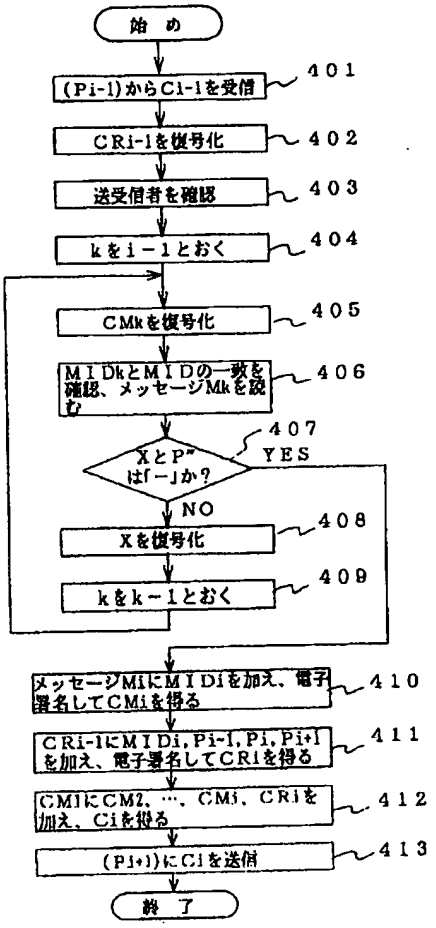
【図12】

図 12


始 め
(Pi)がCiを作成
501
(Pi)が暗号鍵を生成、Ciを暗号化してCi'を得る
502
(Pi)が(Pi+1)にCi'を送る
503
(Pi+1)がCi'に電子署名してCi"を得る
504
(Pi+1)が(Pi)にCi"を返送
505
(Pi)がCi"を復号化
506
(Pi)が復号結果とCi'の一致を確認、(Pi+1)にKiを送る
507
(Pi)がCi"とKiを保管
508
(Pi+1)がCi'を復号化
509
(Pi+1)がCiを得る
510
終 了

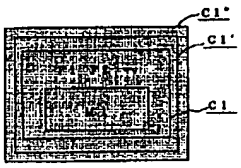
【図11】

図11



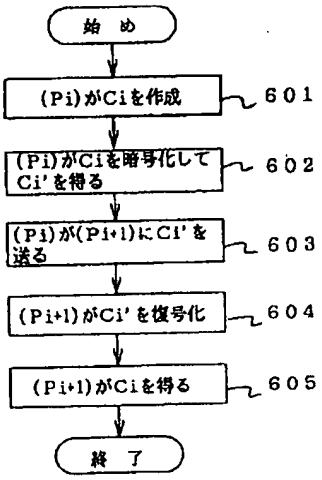
【図13】

図13



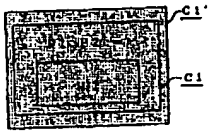
【図14】

図14



【図15】

図15



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI	技術表示箇所
G06F 17/60				